(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/91374 A1

(51) International Patent Classification[7]: H04L 12/26, 12/56, 29/06, H04Q 11/04

(21) International Application Number: PCT/SE01/01144

(22) International Filing Date: 22 May 2001 (22.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0001930-7 24 May 2000 (24.05.2000) SE

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-126 25 STOCKHOLM (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WALLINDER, Sören** [SE/SE]; Skansvägen 14, S-136 70 HANINGE (SE). **BJÖRNSSON, Stefan** [SE/SE]; Baltzars väg 5, S-149 45 NYNÄSHAMN (SE). **LINDBERG, Niclas** [SE/SE]; Vattenledningsvägen 91, S-126 35 HÄGERSTEN (SE).

(74) Agents: **ALBIHNS STOCKHOLM AB** et al.; P O Box 5581, S-114 85 STOCKHOLM (SE).

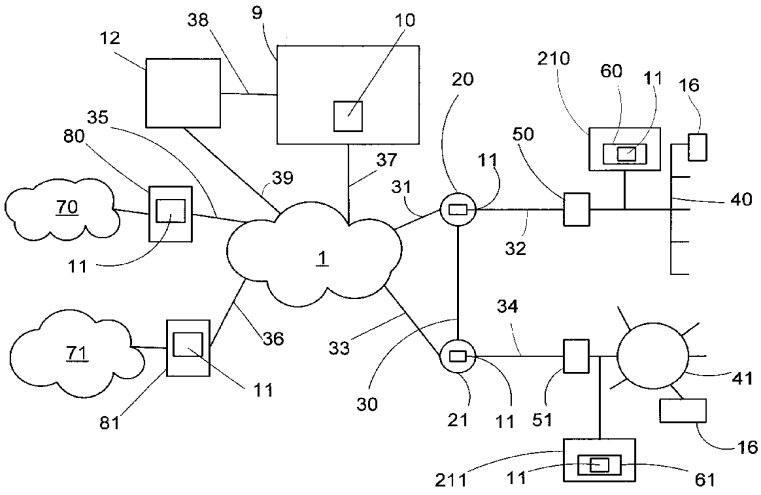
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR INTERCEPTING PACKETS IN A PACKET-ORIENTED NETWORK



(57) Abstract: The invention relates to a method, a system, a node (9), a router (20, 21), a gateway (80, 81), a monitoring means (12), an agent apparatus, an agent computer program (60, 61), an interception computer program (11) and an interception control computer program (10) for intercepting packets in a packet-oriented network (1). The interception comprises the steps of: providing at least one interception means for intercepting and copying information from a packet being transmitted in the network;activating an interception control means (10) for controlling the interception means (11); initiating communication between the interception control means (10) and the monitoring means (12) for monitoring the copied information from the packet; establishing a connection between the interception control means (10) and the interception means (11); ordering the interception means (11) to copy the information; and transmitting the copied information to the monitoring means (12).

WO 01/91374 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR INTERCEPTING PACKETS IN A PACKET-ORIENTED NETWORK

Technical Field of the Invention

The present invention relates to a method, a system, a node, a monitoring means, a router, a gateway, an agent apparatus, an agent computer program, an interception computer program and an interception control computer program for intercepting packets in a packet-oriented network.

Description of Related Art

In many countries the law enforcement personnel conducts court authorised electronic lawful interception (also called wiretapping) of target telephone calls in order to prevent crimes. Therefore many telephone operators need to be able to perform the lawful interception on behalf of the authority. However, the technical progress and common utilisation of packet-oriented networks, such as a TCP/IP-network, also require intercepting and monitoring signals associated with packet transfers. Therefore also internet service providers on behalf of the authority require means to conduct lawful interception in packet oriented networks. A major difference between lawful interception in traditional circuit switched telephone networks and packet oriented networks is that the packet oriented networks have a strict separation between control signalling and media stream, such as Real Time Protocol (RTP) packets. Because of this separation, the control signalling and the media stream usually have different routes in the packet-oriented network.

WO-99/55062-A1 discloses a method and system for intercepting and monitoring signals associated with a telephone number in a communication network. The communication network could be a TCP/IP-network capable of supporting Voice over Internet Protocol (VoIP), according to the description. The network comprises switching nodes, where one of the switching nodes is connected to a collection node for interception. When a first switching node identifies a telephone number belonging

to a person that is to be intercepted (also called a target), a trigger sends a signal to a signal transmission node, which then orders the first switching node to send the data from the target to a second switching node, which is connected to the collection node. All the data - no matter what kind of data it is – sent by a target is transmitted to and replicated by the collection node before the data further is transmitted to a third switching node, which is a controlling node for a fax machine, telephone, desktop computer and a video transmitter/receiver. Thus the signals that are to be intercepted must be transmitted a different way to the receiver than if the signals were not intercepted. Means for intercepting and monitoring signals triggered by e.g. accessing certain internet homepages and e-mail addresses as well as any means for identifying certain data packets are not disclosed.

Summary

It is a general object of the present invention to provide a method and means for performing lawful interception of packets in a packet-oriented network as well as providing a highly flexible system that easily can be implemented in the network.

It is also a general object of the present invention to provide a system that does not force a media stream to and from a target to be routed to a separate node that is connected to a collection node, since this delays the media stream.

The present invention therefore provides a method for intercepting packets in a packet-oriented network, comprising the steps of: providing at least one interception means for intercepting and copying information from a packet being transmitted in the network; activating an interception control means for controlling the at least one interception means; initiating communication between the interception control means and at least one monitoring means for monitoring copied information from the packet; establishing a connection between the interception control means and at least one of the at least one interception means; ordering the one of at least one interception means to copy the information by transmitting a signal from the interception control means;

and transmitting the copied information to the at least one monitoring means. Hereby a flexible and easily implemented method for lawful interception of packets is achieved, thus giving the possibility to make a lawful interception on e.g. multipart video communications, e-mails, chat, computer programs, movies, music files and picture files.

Preferably the method comprises the steps of: providing information about a user identity to the interception control means, which analyses the user identity to determine if a packet related to the user identity is to be intercepted, and identifying the type of the packet, where the identification of the type of the packet is done by at least one of the interception control means, the at least one interception means, and the at least one monitoring means.

Furthermore, the method may comprise the step of installing the at least one interception means in a router in the network, in an agent apparatus for simplifying firewall definitions and terminating communication between a local-area network and another network, or in a gateway. Hereby is achieved that the number of interception means and their positions may be selected in order to achieve a custom made solution for an effective lawful interception.

The one of the at least one interception means may directly transmit the copied information to the at least one monitoring means or to the interception control means, which then transmits the copied information to the monitoring means. This also gives a method that gives several possible ways of performing the lawful interception. The reason for transmitting copied information first to the interception control means is for instance to filter the copied information and/or changing the copied information to another format before it is sent to the monitoring means.

Since the method involves transmission of sensitive information, the method may comprise the step of encrypting the copied information before it is transmitted to the at least one monitoring means or the interception control means. The method may also

comprise the step of encrypting any interception related information, e.g. being transmitted between the interception control means and the at least one monitoring means. Hereby is achieved that if someone for some reason eavesdrop the information being transmitted between the interception control means, the interception means and the monitoring means, will find it impossible to understand.

The interception related information may comprise time data for identifying the beginning, end and duration of a connection between two user identities.

In order to have a list of user identities that are targets at few places as it is sensitive information, the method may comprise the step of storing at least one user identity, whose communication with other user identities shall be intercepted, in the interception control means.

Suitably, the method may comprise the step of transmitting information about the addresses of communicating user identities, whose communication is to be intercepted, and the address of the at least one monitoring means from the interception control means to the at least one of the at least on interception means. Hereby is achieved that the interception function knows where to send the copied information and which packets that are going to be intercepted.

The present invention also relates to an interception system for intercepting packets in a packet-oriented network, comprising at least one interception means for intercepting and copying information from a packet being transmitted in the network, an interception control means intended for installation in a node in the network for controlling the at least one interception means and at least one monitoring means for monitoring copied information being transmitted from the at least one interception means and communicating with the interception control means. Hereby a system for performing the above mentioned method is achieved.

Suitably, the interception means in the interception system is adapted to be installed in a router and/or a gateway and/or an agent apparatus. The copied information from the interception means could be sent directly to the monitoring means or to the control means, which then transmit the copied information to the monitoring means.

In one embodiment an embodiment of the interception system, the one of the at least one interception means is installed in the node, which may be a service node, a gateway, an agent apparatus or a router. Suitably the one of the at least one interception means comprises a program module stored in a first memory means associated with a first processing unit and a main part stored in a second memory means associated with a second processing unit. The interception control means may also comprise a program module stored in the first memory means associated with a first processing unit and a main part stored in the second memory means associated with the second processing unit. Hereby is achieved that the interception system requires less capacity from a main CPU, which means that the main CPU may be used more effectively for other tasks, such as routing of packets and proxy server performance.

Furthermore, the present invention relates to a node in a packet-oriented network, comprising an interception control means adapted for controlling at least one interception means for intercepting packets in the network, and a first port adapted for connecting the interception control mean with a monitoring means for monitoring intercepted information. Hereby is achieved that for example a service node with the interception control means may be provided to service providers. Also, it is achieved that a monitoring means for a law enforcement agency may be connected to the node in order to get interception related information. The node may also comprise a second port for sending and receiving information from the at least one interception means.

Preferably, at least one user identity, whose communication with other user identities shall be intercepted, is stored in the interception control means in the node.

Also, one of the at least one interception means may be installed in the node and comprise a program module stored in a first memory means associated with a first processing unit and a main part stored in a second memory means associated with a second processing unit. The interception control means may also comprise a program module stored in the first memory means associated with the first processing unit and a main part stored in the second memory means associated with the second processing unit.

Moreover, the present invention relates to a monitoring means for monitoring copied information from an intercepted packet in a packet-oriented network. The monitoring means comprises a port intended for connecting the monitoring means with an interception control means for controlling at least one interception means and transmitting interception related information, such as a call identifier, user identities, addresses associated with the user identities and service information, to the monitoring means. Hereby is achieved that a monitoring means for monitoring information from a lawful interception may be provided to the law enforcement agency.

Suitably the monitoring means comprises recording means and at least one display means for recording and displaying information sent by either the interception control means or an interception means for intercepting and copying information in the packet. Hereby is achieved that law enforcement personnel is able to see directly the media transfer to and from a target and take different measures depending on what might be seen.

The monitoring means suitably comprises communication means to transmit acknowledgements or requests to the interception control means.

The present invention also relates to a router intended for a packet-oriented network. The router comprises an interception means for intercepting and copying information from a packet being transmitted in the packet-oriented network and an interception control means for controlling the interception means, the interception means

comprising a program module stored in a first memory means associated with a first processing unit and a main part stored in a second memory means associated with a second processing unit and the router is adapted to be connected to at least one monitoring means for monitoring copied information from the packet, where the copied information is transmitted by the interception means directly to the monitoring means or through the interception control means. Hereby is achieved that a router with the interception means may be installed at strategic intercept positions in a packet-oriented network.

The interception control means may also comprise a program module stored in the first memory means associated with the first processing unit and a main part stored in said second memory means associated with the second processing unit.

The present invention also relates to a gateway between at least two networks of which at least one is a packet-oriented network. The gateway comprises an interception means for intercepting and copying information from a packet being transmitted in the packet-oriented network, and an interception control means for controlling the interception means. The gateway is adapted to be connected to at least one monitoring means for monitoring copied information from the packet, the copied information being transmitted by the interception means directly to the monitoring means or through the interception control means. The interception means comprise a program module stored in a first memory means associated with a first processing unit and a main part stored in a second memory means associated with a second processing unit. Hereby is achieved that a gateway with the interception means may be installed between two different networks where at least one is a packet-oriented network. The gateway is intended to be connected to at least one monitoring means for monitoring copied information from the packet, where the copied information is transmitted by the gateway directly to the monitoring means or through the interception control means.

The interception control means in the gateway may comprise a program module stored in the first memory means associated with the first processing unit and a main part stored in the second memory means associated with the second processing unit.

The present invention also relates to a first embodiment of an agent apparatus in a packet-oriented local-area network. The agent apparatus comprises an interception means for intercepting and copying information from a packet being transmitted in the network, and a port adapted to connect the agent apparatus with an interception control means for controlling the interception means. The agent apparatus is also adapted to be connected to at least one monitoring means for monitoring copied information from the packet, where the copied information is transmitted by the agent apparatus directly to the monitoring means or through the interception control means. Hereby is achieved that an interception with the interception system and method could be done in a local-area network.

In addition, the invention relates to a second embodiment of an agent apparatus in a packet-oriented local-area network. The second embodiment of the agent apparatus comprises an interception means for intercepting and copying information from a packet being transmitted in the packet-oriented local-area network and an interception control means for controlling the interception means. The interception means comprises a program module stored in a first memory means associated with a first processing unit and a main part stored in a second memory means associated with a second processing unit and the agent apparatus is adapted to be connected to at least one monitoring means for monitoring copied information from the packet, where the copied information is transmitted by the interception means directly to the monitoring means or through the interception control means.

The present invention also relates to an agent computer program in a local-area network. The agent computer program comprises computer readable code means for simplifying firewall definitions and terminating communication between the local-area network and another network. The agent computer program further comprises an

interception computer program comprising computer readable code means configured to cause an interception and copying of information in a packet being transmitted in the local-area network, and computer readable code means configured to allow communication between the interception computer program and an interception control computer program for controlling the interception computer program. The interception computer program comprises computer readable code means configured to cause a transmission of copied information to a monitoring means for monitoring the copied information. Alternatively the interception computer program comprises computer readable code means configured to cause a transmission of copied information to said interception control computer program. Related to this, a computer program product comprising a computer useable medium and the agent computer program, said agent computer program being recorded on the computer useable medium. Hereby is achieved that the agent computer program may be distributed to different LANs in order to improve the possibilities for an effective lawful interception.

The invention also relates to the interception computer program described above. Also provided is a computer program product, comprising a computer useable medium and the interception computer program, said interception computer program being recorded on the computer useable medium. Hereby is achieved that the interception computer program may be installed in different devices in order to provide the method and devices mentioned above. In an embodiment of the interception computer program not described in conjunction with the agent computer program, the interception computer program comprises a program module, which is adapted to be stored in a first memory means associated with a first processing unit, and a main part adapted to be stored in a second memory means associated with a second processing unit, where the program module comprises the computer readable code means configured to cause an interception and copying of information in the packet being transmitted in the communications network and the main part comprises the computer readable code means configured to allow communication between the interception computer program and the interception control computer program.

The invention also relates to an interception control computer program comprising:
computer readable code means configured to cause a controlling of an interception computer program, which intercept and copy information in a packet being transmitted in a packet-oriented network;
computer readable code means configured to enable communication between the interception control computer program and a monitoring means for monitoring copied information from the packet;
computer readable code means configured to enable communication between the interception control computer program and a node; and
computer readable code means configured to cause an order to the node or the interception computer program to prevent or terminate communication between user identities where one of the user identities is stored in the interception control computer program.

Hereby is achieved that an interception control computer program may be provided to service providers that use a packet-oriented network. Also the traffic associated with a person, whose communication in the network is to be intercepted, may be terminated in case of e.g. information comprising instructions to launch non governmental missiles.

Suitably the interception control computer program comprises a computer readable code means configured to cause a transmission of interception related information, such as a call identifier, user identities, addresses associated with the user identities and service information, to the monitoring means.

Moreover, the interception control computer program preferably comprises computer readable code means configured to enable a storage of at least one user identity, whose communication with other user identities shall be intercepted, in the intercept control computer program.

Advantageously, the interception control computer program comprises computer readable means configured to cause a positive or negative answer to an interception request from the node of whether a packet related to a user identity connected to the node shall be intercepted.

Suitably, the interception control computer program comprises computer readable means configured to cause a reception of the copied information transmitted by the interception computer program and then transmitting the copied information to the monitoring means.

The interception control computer program preferably comprises computer readable means configured to cause a stop signal, which is being transmitted to said intercept control computer program in order to stop the interception and copying of the packet. Hereby is achieved that court orders that only allow a lawful interception of a certain type of service can be followed when an intercepted service stops and the target starts to use another service. The stop signal is also used when a target logs out from the packet-oriented network.

Because of the sensitive information sent, the interception control computer program comprises computer readable means configured to cause encrypting of all information that is transmitted by the interception control computer program.

The interception control computer program may in one embodiment comprise a program module, which is adapted to be stored in a first memory means associated with a first processing unit, and a main part adapted to be stored in a second memory mean associated with a second processing unit, where said program module comprises a part of said computer readable code means and the rest of said computer readable code means is comprised in said main part.

Related to the interception control computer program, a computer program product is provided, which comprises a computer useable medium and the interception control

computer program, where said interception control computer program is recorded on the computer useable medium.

Brief Description of the Drawings

The objects, advantages and effects as well as features of the present invention will be more readily understood from the following detailed description of a preferred embodiment of the invention, as well as other embodiments, when read together with the accompanying drawings, in which:

Fig. 1 shows a schematic block diagram of a first embodiment of the invention;
Fig. 2 shows a schematic diagram of a first embodiment of a service node;
Fig. 3 shows an example of a monitoring means according to the invention;
Fig. 4 shows a schematic diagram of an embodiment of a router;
Fig. 5 shows a schematic diagram of an embodiment of a gateway;
Fig. 6 shows a schematic diagram of an embodiment of an agent apparatus;
Fig. 7 shows a flow diagram of a set-up of a lawful interception when a target is calling;
Fig. 8 shows a flow diagram of a set-up of the lawful interception when a user is calling the target; and
Fig. 9 shows a second embodiment of a node according to the invention.

Detailed Description of Embodiments

While the invention covers various modifications and alternative methods and systems, suitable embodiments of the invention are shown in the drawings and will hereinafter be described in detail. It is to be understood, however, that the specific description and drawings are not intended to limit the invention to the specific form disclosed. On the contrary, it is intended that the scope of the claimed invention includes all modifications and alternative constructions thereof falling within the spirit

and scope of the invention as expressed in the appended claims to the full range of their equivalents.

After a court order to a law enforcement agency (LEA) to conduct lawful interception associated with, for example, a person, also called a target. The LEA then gives the lawful authorisation to a service provider, such as an internet service provider. The service provider determines the relevant target identities from the information given by the LEA and prepares interception devices for the lawful interception.

Fig. 1 shows a block diagram giving an overall view of a preferred embodiment. A packet-oriented network 1, such as an Internet Protocol backbone with routers, is mainly shown only as a cloud-shaped block for the ease of understanding. Here only a first and a second router 20 and 21 are seen connected to the rest of the packet-oriented network 1, but of course more routers connected to the packet-oriented network 1 could have been shown. A first, second and third link, 30, 31 and 32, are connected to the first router 20 and the first link 30, a fourth and a fifth link, 33 and 34, are connected to the second router 21, but of course there could be any number of links to the routers 20, 21. The first router 20 is connected to a first local-area network (LAN) 40 , such as an Ethernet based network, and the second router is connected to a second LAN 41, for example a token ring network. A first firewall 50 associated with the first LAN 40 is installed between the first LAN 40 and the first router 20 in order to prevent unauthorised access to or from the first LAN 40. For the same purpose, a second firewall 51 associated with the second LAN 41 is installed between the second LAN 41 and the second router 21. In the first LAN 40, a first agent 60 works like a proxy server that is used as a part of the LAN 40 to simplify firewall definitions and to terminate transport layer communication between untrustworthy outside networks and the LAN 40 protected by the firewall 50. The first agent 60 is installed in a first agent apparatus 210, i.e. a proxy server hardware. In the same way, LAN 41 has a similar second agent 61, which is installed in a second agent apparatus 211. Any device, such as workstations, personal computers, and cameras, known to be connectable to a LAN

may of course be connected to each one of the first LAN 40 and the second LAN 41. Here only one such device in each LAN is shown, represented by blocks 16.

Also shown in fig. 1 are a first telephone network 70 and a second telephone network 71, such as public switched telephone networks (PSTN) or public land mobile networks (PLMN). A first gateway 80, in the form of a voice gateway that interfaces and translates, is installed between the packet-oriented network 1 and the first telephone network 70 in order to transmit signals from for example a PSTN to another PSTN through the packet-oriented network 1, i.e. using an IP-telephone system. A sixth link 35 connects the packet-oriented network 1 to the first gateway 80. In a similar way, the second telephone network 71 are connected to the packet-oriented network 1 through a seventh link 36 and a second gateway 81.

A service node (SN) 9 is connected to the packet-oriented network 1 by an eighth link 37. In case of, for example, an IP-telephone system, the SN 9 comprises: a user agent (UA), a service agent (SA), a sitekeeper (SK) and an application programming interface to higher layer applications such as voice mail, e-mail convergence and web-initiated dialling, or vertical applications such as sales support, customer care systems, and order and logistics systems. The SK controls access agents, i.e. gateways and agents as the first agent 60 and the second agent 61, for a site. Incoming traffic from an originating access agent is routed by the SK towards the destination. The traffic is addressed towards any of the access agents in the terminating site that supports the dialled number. The UA is responsible for user oriented call services and handles user authentication, authorisation, accounting and SA invocation. A user of an IP-telephone system is assigned to a UA that is used each time the user makes a call in the IP-telephone system regardless of the user location in the network. The SA is responsible for supplementary services and communicates with the UA. Also, the SA provides a service creation environment (SCE) which is a high level abstraction application program interface (API) that allows easy service development. The SCE may be used to implement the interception devices. In the ITU-T standard, known to a person skilled in the art, the SA, UA and SK are comprised in the so-called gatekeeper.

The interception devices comprise an interception control means (ICM) 10, interception means (IM) 11 and a monitoring means (MM) 12. In the preferred embodiment of the invention, the ICM 10 is an interception control computer program product – a logical function with preferably all the logic to perform the lawful interception and control the IM 11, which preferably also is a logical function. Preferably, the ICM 10 is installed in the SN 9, but may be positioned in any other place in the packet-oriented network 1. In the SN 9, the ICM 10 is preferably attached to the SA since all service related information is stored there and since the SA has an interface towards the UA for retrieving user specific information. There may be several IMs 11 distributed in the packet-oriented network 1 as an installed part of a router, such as the routers 20 and 21. Alternatively, or in addition, the IM 11 may also be implemented in gateways, such as the first and the second gateways 80 and 81 and/or in agents such as the first agent 60 and the second agent 61. The distribution and the number of the IMs 11 are a strategic matter since the media stream that is to be intercepted must pass at least one IM 11 and a target must not understand that his/her communication is delayed because it has to be transmitted a long and/or slow way to an IM. It is also possible to install IMs in endpoints, such as terminals, but a skilled user would then easily know that he/she is being intercepted. The ICM 10 keeps track of the IM 11 and may direct copied content information (CI) sent by a user to the nearest MM 12. The CI is the media stream, e.g. speech or data, that is intended to be sent to one user from another user. When the interception is going to be performed the ICM 10 orders the IM 11 to start the interception, duplicate the intercepted media stream and transmit the duplicated media stream to the MM 12, either directly without passing the ICM 10 or by first passing the ICM 10. The ICM 10 also stops the interception and handles the communication with other means. Information about users that are targets for the interception may be stored in the ICM 10. Also, it is possible to intercept several calls, file transfers etc. at the same time and the ICM 10 controls every interception being in progress. Furthermore, the ICM 10 collects and forwards interception related information (IRI) about the intercepted target to the MM 12. The IRI for the communication is associated with the services that the target

utilises and may comprise e.g. the user identities that have successfully or unsuccessfully attempted to communicate with the target; the user identities that the target have successfully or unsuccessfully attempted to communicate with; details of services used and their associated parameter; and time-stamps for identifying the beginning, end and duration of the connection. Although only one ICM 10 is shown in fig. 1, there may be several ICMs connected to the packet-oriented network 1, preferably in one SN each, where the SNs may be owned by different service providers.

The MM 12 is provided by the LEA and collects and displays all the IRI and copied CI that the ICM 10 transmits through an ninth link 38 or one of the IMs 12 transmits through a tenth link 39 without passing the ICM 10. The communication between the MM12 and the ICM 10 may be a two-way communication, whereas the communication through the tenth link 39 only is from the IMs 11 to the MM 12. The reason for this is that all the control means for the lawful interception is in the ICM 10. There may of course be more than one MM 12, as it may be appropriate to have MMs geographically distributed in order to provide proper availability to the intercepted information for the law enforcement personnel.

Fig. 2 shows a schematic view of the SN 9, which comprises a central processing unit (CPU) 130, buses 140, a memory means 150, a first port 170 for connecting the SN 9 with the monitoring means 12, and a second port 171 for the eighth link 37. The CPU 130 processes all the tasks of the SN 9 with the help of the buses 140 and the memory means 150, which comprises the UA, SK, SA, and ICM 10. The memory means may be e.g. a hard disk, a read-only memory a flash memory or the like.

Fig. 3 shows an example of the MM 12. Here the MM 12 comprises a computer terminal with a display means 18 in the form of a display screen and a box 19. The box 19 comprises buses 141, a recording means in the form of a hard disk drive 151, a communication means in the form of a CPU 131, a port 172 intended for connecting the monitoring means 12 with the SN 9, and a port 173 for communication with the

display means 18. Also shown is a computer useable medium in the form of a floppy disk 200.

Fig. 4 shows a schematic diagram of a router according to the invention. Here the router is exemplified by the first router 20, which comprises a CPU 132, a memory means 152, ports 174 for connection with the first, second and third link 30, 31, and 32, and buses 142 enabling communication between the memory means 152, the ports 174 and the CPU 132. The memory means 152 comprises the IM 11.

Fig. 5 shows a schematic diagram of a gateway according to the invention. Here the gateway is exemplified by the first gateway 80, which comprises a CPU 133, a memory means 153, a first port 175 for connecting the gateway 80 to the first telephone network 70, a second port 176 and buses 143. The buses enable communication between the memory means 153, the CPU 133, the first port 175 and the second port 176. The second port 176 is intended for connecting the gateway to the packet-oriented network 1 and the ICCM 10 in the SN 9. The memory means 153 comprises the IM 11. It should be noted that this configuration is also applicable to any other so-called boarder element between two networks where one is a packet-oriented network.

Fig. 6 shows a schematic diagram of an agent apparatus, a proxy server apparatus etc. according to the invention. Here the agent apparatus is exemplified by the first agent apparatus 210, which comprises a CPU 134 for communication and execution of the agent 60, a memory means 154, a port 177 for connecting the agent apparatus with the rest of the LAN 40, and buses 144. The buses enable communication between the memory means 154, the CPU 134 and the port 177. The memory means 154 comprises the agent 60, which comprises the IM 11.

Now six communication examples using a packet-oriented network will be described. Each one of them may be intercepted by the above described interception devices.

The first example is a call from a user in either the first telephone network 70 or the second telephone network 71 to a user in a IP-telephone system in either the first LAN 40 or the second LAN 41. If the call is done from the first telephone network 70 to the first LAN 40, the media stream will go through the first gateway 80, the sixth link 35, the second link 31, the router 20, the third link 32 and the firewall 50 and then maybe treated by the first agent 60 before it reaches the receiving user in the first LAN 40. The interception point for the IM 11 is here preferably in the first gateway 80 or in the first agent 60.

The second example is a call from a user in a IP-telephone system, in for example the first LAN 40 or the second LAN 41, to a user in another system, such as one of the first telephone system 70 or the second telephone system 71 using a PSTN or PLMN system. If the call is done from the second LAN 41 to the second telephone network 71, the media stream will pass through the second agent 61, the second firewall 51, the fifth link 34, the fourth link 33, the seventh link 36, the second gateway 81 before it reaches the receiving user in the second telephone network 71. The interception point for the IM 11 is here preferably in the second agent 61 or in the second gateway 81.

The third example is a call from a user in a telephone system to another user in another telephone system, where the systems themselves are not IP-telephone systems, but which are connected to each other by a packet-oriented network. If a call is done from the first telephone system 70 to the second telephone system 71, the media stream will pass through the first gateway 80, the sixth link 35, the packet-oriented network 1, the seventh link 36, the second gateway 81 before it reaches the receiving user in the second telephone network 71. The interception point for the IM 11 is here preferably in the first gateway 80 or in the second gateway 81.

The fourth example is for example a call, an e-mail, a file transfer or a video conference data transfer from a user in a segment in a packet-oriented network to a user in another segment of the packet oriented network. For example an IP-telephone call from the first LAN 40 to the second LAN 41 leads the media stream through the

first agent 60, the first firewall 50, the third link 33, the first router 20, the first link 30 or the second link 31 and the fourth link 33, the second router 21, the fifth link 34, the second firewall 51 and the second agent 61 in the second LAN 41. The interception point for the IM 11 is here preferably in the first agent 60 or in the second agent 61.

The fifth example is for example a call, an e-mail, a file transfer or a video conference data transfer from a user in a segment of a packet-oriented network to a user in the same segment of the packet-oriented network. An example is a LAN, such as the first LAN 40, supporting IP-telephony, where a user in that LAN calls another user in the same LAN. The interception point for the IM 11 in the first LAN 40 is preferably in the first agent 60, which the media stream has to pass. Of course the interception point for the IM 11 might be in one of the end points, but as said before, a skilled user will then easily know that he/she is intercepted.

The sixth example is multipart communication, e.g. a multipart speech service or a multipart video conference service provided by a service provider to users in different networks or different segments of a network. A conversation between a user in the first LAN 40, a user in the second LAN 41, a user in the first telephone network 70 and a user in the second telephone network 71 may be intercepted in the first gateway 80, the second gateway 81, the first agent 60 or the second agent 61.

Another example of placing the IM 11 is in a node somewhere in the packet-oriented network, preferably a centrally placed node, and directing all traffic that is to be intercepted through the IM 11 in that node. This allows for interception in all five of the above mentioned communication examples, but may generate unacceptable medial stream delays.

An example of the interaction between different nodes and the interception devices during the set-up when the target makes a call, will now be described with the help from Fig. 7. First there is an installation of the MM 12 as a node, installation of the ICM 12 in the SN 9 and installation of at least one IM 11 in for example a router, a

gateway or an agent means that works like a proxy server. Then the ICM 12 gets information of a user identity, which is stored as "active" in the ICF. The user identity may be e.g. a telephone number, an e-mail address, a website address, an IP-address, an International Mobile Equipment Identifier (IMEI) or International Mobile Station Identity (IMSI). In Fig. 6, the target calls from device 16 in the first LAN 40 and there are eleven principal steps S1-S11, where S1 is the first step and the other follow after each other in sequence according to their number.

Step S1: The target makes a service request from the device 16, e.g. a telephone, a fax machine or a computer. A set-up signal goes from the device 16 to the first agent 60.

Step S2: The first agent 60 routes the call to its SK.

Step S3: The SK routes the call to the SN 9 of the target.

Step S4: The SN 9 makes an interception request to the ICM 10 to find out if the interception shall be performed.

Step S5: The ICM 10 finds out that the user is a target and responds with a positive answer. The positive answer is triggered by the user identity.

Step S6: The ICM 10 sends the address of the IMs 11 to the SN, as well as giving orders to initiate the services requested by the target. Alternatively the ICM 10 could deny the request of the target if it for some reason is a court order for that.

Step S7: The SN sends back an acknowledgement to the ICM 10.

Step S8: The ICM 10 sends information about an interception to a suitable IM 11. The information comprises the addresses of the communicating users and the address to a suitable MM 12.

Step S9: The IM 11 sends an acknowledgement back to the ICM 10.

Step S10: The ICM 10 sends IRI to the MM 12 that there will be an interception and that the MM 12 should be prepared to receive copied intercepted CI either from the IM 11 or from the ICM 10. The IRI will contain e.g. call identifier, address of the non calling user/users and the target, and service information.

Step S11: The MM 12 sends an acknowledgement back to the ICM 10. Thereafter the IM 11 starts to copy the CI and sends it to the MM12 or the ICM 10.

If a user calls the target there is another procedure after the installation of the interception devices and the activation of a target. In Fig. 7, a user calls the target in for example the first LAN 40 from a device 16 in the second LAN 41. Here there are sixteen principal steps S21-S36 to set-up the lawful interception, where S21 is the first step and the other follow after each other in sequence according to their number.

Step S21: The user makes a call from his device 16. A set-up signal goes from the terminal to the second agent 61.

Step S22: The second agent 61 routes the call to its SK, here called the first SK.

Step S23: The first SK sends information about the calling user identity to the belonging SN, here called the first SN.

Step S24: The first SN makes an interception request to the ICM 10 to find out if an interception shall be performed.

Step S25: The answer of the ICM 10 is negative and the answer is sent back to the first SN.

Step S26: The answer is forwarded to the first SK.

Step S27: The originating side, here device 16, sends a set-up signal comprising the calling user identity and the target user identity to a second SK associated with the target.

Step S28: The second SK sends a set-up signal to a second SN associated with the second SK. If the user and the target belong to the same SN, the second SN is of course the same as the first SN.

Step S29: The second SN makes an interception request to a second ICM belonging to the second SN.

Step S30: The second ICM finds out that the receiver of the call is a target and responds with a positive answer. Information about the address of a suitable IM 11 is sent to the second SN.

Step S31: The second ICM orders an initiation of the requested service of the user in LAN 41. Alternatively, the second ICM could deny communication with the target if it is a court order for that.

Step S32: The second SN sends back an acknowledgement.

Step S33: The second ICM sends information about an interception to a suitable IM 11. The information comprises the addresses of the communicating users and the address to a suitable IM 11.

Step S34: The IM 11 sends an acknowledgement to the second ICM.

Step S35: The second ICM sends IRI to the MM 12 that there will be an interception and that the MM 12 should be prepared to receive copied intercepted CI either from

the IM 11 or from the second ICM. The IRI shall contain e.g. call identifier, address of the calling user and the target, and service information.

Step S36: The MM 12 sends an acknowledgement back to the second ICM and the IM 11 starts to copy the CI and sends it to the MM 12 or the second ICM.

When the communication has ended or when the controlling ICM decides to break the lawful interception, the ICM sends a last message with IRI to the MM, which sends an acknowledge back to the ICM, which thereafter ends the communication with the MM. The ICM also orders the active IM to stop intercepting possible CI and stop transmitting copied CI to the ICM or the MM. Thereafter the communication between the ICM and the active IM is ended.

Since the communication between the ICM 10, the IMs 11 and the MM 12 is secret, any communication between them may be encrypted such that no unauthorised person should be able to understand the copied CI or the IRI. To understand the encrypted information at least the MM 12 must comprise a means for reverse the encrypted information back to the original information.

The processing associated with lawful interception has been tested in some systems and measurements of the amount of the processing power allocated for the lawful interception, including the determining of whether an interception shall be performed, have shown that up to a quarter of the processing capacity may have to be allocated for processing associated with the interception although an interception currently is not being performed. This makes the processing capacity less for other tasks such as routing packets. The routing of packets may thus be slower than it would be without the interception feature. Fig. 9 shows a second embodiment of at least a part of a node 22 in the packet-oriented network 1, although explicitly not shown in Fig. 1. The node may be a router, a gateway, an agent apparatus or a service node of the same principal features as disclosed earlier in the description. However, in this embodiment the node comprises both the ICM 10 and the IM 11. In order to increase the capacity of the node

for its main tasks, such as routing packets in the case where the node is a router, both the ICM 10 and the IM 11 comprise two separate parts comprised in different memory means, e.g. hard disks, read-only memories or flash memories. Compared to the previous embodiments of the different nodes, this embodiment comprises at least one additional, second processing unit 230, which main purpose is to process most of the traffic related to the lawful interception. Hence, a first processing unit 240, which mainly handles the main traffic to and from the node, such as the CPU:s 130-134, is supervised by the second processing unit 230 such that the interception requires less processing by the first processing unit 240. Suitably, as little as necessary of the ICM 10 and the IM 11 respectively is stored in first memory means 250 and 251 respectively and is processed by the first processing unit 240; the rest of the ICM 10 and the IM 11 is stored in second memory means 252 and 253 respectively, said second memory means 252 and 253 being connected to the second processing unit 230. The second processing unit 230 is in this embodiment positioned on a different printed circuit card, which may be comprised in the same unit as the first processing unit 240 or comprised in an additional server unit, which also is comprised in the node. In other words, each one of the ICM 10 and the IM 11 may comprise a main part, 10' and 11' respectively, being processed by the second processing unit 230 and a smaller program module, 10" and 11" respectively, which is processed by the main processing unit 240. The smaller program module 11" of the IM 11 may substantially only comprise code means for a packet sniffer function and for communication with the main part 11' of the IM 11, whereas the main part 11'of the IM 11 comprises the code means for e.g. starting and stopping the interception upon request from the ICM 10 and forwarding copied information to the main part 10' of the ICM 10' or the MM 12. The packet sniffer function is the part of the IM 11 that monitors data travelling over the node 22 and copies selected packets. Although the main part of the ICM and IM in this embodiment is stored in different second memory means, 252 and 253 respectively, it shall be understood that they may be stored in the same memory means, such as the second memory means 252. However, it is important to notice that the ICM 10 and the IM 11 suitably always are logically separated from each other.

Claims

1. A method for interception of packets in a packet-oriented network (1), comprising the steps of:
activating an interception control means (10) for controlling at least one interception means (11) for intercepting and copying information from a packet being transmitted in said network (1);
initiating communication between said interception control means (10) and at least one monitoring means (12) for monitoring copied information from said packet;
establishing a connection between said interception control means (10) and at least one of said at least one interception means (11);
ordering said one of at least one interception means (11) to copy said information by transmitting a signal from said interception control means (10); and
transmitting said copied information to said at least one monitoring means (12).

2. A method according to claim 1, comprising the steps of:
providing information about a user identity to said interception control means (10), which analyses said user identity to determine if a packet related to said user identity is to be intercepted.

3. A method according to claim 1 or 2, comprising the step of identifying the type of said packet.

4. A method according to claim 3, where said identification of the type of said packet is done by at least one of said interception control means (10), said at least one interception means (11) and said at least one monitoring means (12).

5. A method according to anyone of the preceding claims, comprising the step of installing said at least one interception means (11) in a router (20, 21, 22) in said network (1), in an agent apparatus (210, 211, 22) for simplifying firewall definitions

and terminating communication between a local-area network (40, 41) and another network, or in a gateway (80, 81, 22).

6. A method according to anyone of the preceding claims, where said one of said at least one interception means (11) directly transmits said copied information to said at least one monitoring means (12).

7. A method according to anyone of claims 1-5, where said one of said at least one interception means (11) transmits said information to said interception control means (12), which then transmits said copied information to said monitoring means (12).

8. A method according to any one of the preceding claims, comprising the step of encrypting said copied information before it is transmitted to said at least one monitoring means (12) or said interception control means (10).

9. A method according to anyone of the preceding claims, comprising the step of encrypting any interception related information, e.g. being transmitted between said interception control means (10) and said at least one monitoring means (12).

10. A method according to anyone of the preceding claims, where said interception related information comprises time data for identifying the beginning, end and duration of a connection between two user identities.

11. A method according to anyone of the preceding claims, comprising the step of storing at least one user identity, whose communication with other user identities shall be intercepted, in said interception control means (10).

12. A method according to anyone of the preceding claims, comprising the step of transmitting information about the addresses of communicating user identities, whose communication is to be intercepted, and the address of said at least one monitoring

means (12) from said interception control means (10) to said at least one of said at least one interception means (11).

13. An interception system for intercepting packets in a packet-oriented network (1), comprising at least one interception means (11) for intercepting and copying information from a packet being transmitted in said network (1), an interception control means (10) installation in a node (9, 22) in said network (1) for controlling said at least one interception means (11), and at least one monitoring means (12) for monitoring copied information being transmitted from said at least one interception means (11) and communicating with said interception control means (10).

14. An interception system according to claim 13, where one of said at least one interception means (11) is adapted to be installed in a router (20, 21, 22).

15. An interception system according to claim 13 or 14, where one said at least one interception means (11) is adapted to be installed in a gateway (80, 81, 22).

16. An interception system according to anyone of claims 13-15, where one of said at least one interception means (11) is adapted to be installed in an agent apparatus (210, 211, 22).

17. An interception system according to anyone of claims 13-16, where said copied information first is transmitted from said interception means (11) to said interception control means (10), which then transmits said copied information to said monitoring means (12).

18. An interception system according to claim 13, where one of said at least one interception means (11) is installed in said node (22).

19. An interception system according to claim 18, where said node (22) is a gateway, an agent apparatus or a router.

20. An interception system according to claim 18 or 19, where said one of said at least one interception means (11) comprises a program module (11") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (11') stored in a second memory mean (252, 253) associated with a second processing unit (230).

21. An interception system according to claim 18-19, where said interception control means (10) comprises a program module (10") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (10') stored in a second memory mean (252, 253) associated with a second processing unit (230).

22. A node (9, 22) in a packet-oriented network (1), comprising an interception control means (10) adapted for controlling at least one interception means (11) for intercepting packets in said network (1), and a first port (170) adapted for connecting said interception control means (10) with a monitoring means (12) for monitoring intercepted information.

23. A node (9, 22) according to claim 22, where at least one user identity, whose communication with other user identities shall be intercepted, is stored in said interception control means (10).

24. A node (9,22) according to claim 22 or 23, comprising a second port (171) for sending and receiving information from said at least one interception means (11).

25. A node (22) according to anyone of claims 22-24, where one of said at least one interception means (11) is installed in said node (22).

26. An node (22) according to claim 25, where said one of said at least one interception means (11) comprises a program module (11") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (11')

stored in a second memory mean (252, 253) associated with a second processing unit (230).

27. A node (22) according to claim 25, where said interception control means (10) comprises a program module (10") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (10') stored in a second memory mean (252, 253) associated with a second processing unit (230).

28. A monitoring means (12) for monitoring copied information from an intercepted packet in a packet-oriented network (1), comprising a port (172) intended for connecting said monitoring means (12) with an interception control means (10) for controlling at least one interception means (11) and transmitting interception related information, such as a call identifier, user identities, addresses associated with said user identities and service information, to said monitoring means (12).

29. A monitoring means (12) according to claim 28, comprising recording means (131) and at least one display means (18) for recording and displaying information sent by either said interception control means (10) or an interception means (11) for intercepting and copying information in said packet.

30. A monitoring means (12) according to claim 28-29, comprising communication means (131) to transmit acknowledgements or orders to said interception control means (10).

31. A router (22) for a packet-oriented network (1), comprising an interception means (11) for intercepting and copying information from a packet being transmitted in said packet-oriented network (1) and an interception control means (10) for controlling said interception means (11), said interception means (11) comprises a program module (11") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (11') stored in a second memory means (252, 253) associated with a second processing unit (230) and said router is adapted to be connected to at

least one monitoring means (12) for monitoring copied information from said packet, where said copied information is transmitted by said interception means (11) directly to said monitoring means (12) or through said interception control means (10).

32. A router (22) according to claim 31, where said interception control means (10) comprises a program module (10") stored in said first memory means (250, 251) associated with said first processing unit (240) and a main part (10') stored in said second memory means (252, 253) associated with said second processing unit (230).

33. A gateway (22) between at least two networks of which at least one is a packet-oriented network (1), comprising an interception means (11) for intercepting and copying information from a packet being transmitted in said packet-oriented network (1), and an interception control means (10) for controlling said interception means (11), where said gateway (22) being adapted to be connected to at least one monitoring means (12) for monitoring copied information from said packet, said copied information being transmitted by said interception means (11) directly to said monitoring means (12) or through said interception control means (12) and said interception means (11) comprises a program module (11") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (11') stored in a second memory means (252, 253) associated with a second processing unit (230).

34. A gateway (22) according to claim 33, where said interception control means (10) comprises a program module (10") stored in said first memory means (250, 251) associated with said first processing unit (240) and a main part (10') stored in said second memory mean (252, 253) associated with said second processing unit (230).

35: An agent apparatus (210, 211, 22) in a packet-oriented local-area network (40, 41), comprising an interception means (11) for intercepting and copying information from a packet being transmitted in said packet-oriented local-area network (40, 41), and a

port (177) adapted to connect said agent apparatus (210, 211) with an interception control means (10) for controlling said interception means (11).

36. An agent apparatus (210, 211) according to claim 29, where said agent apparatus (210, 211) is adapted to be connected to at least one monitoring means (12) for monitoring copied information from said packet, where said copied information is transmitted by said agent apparatus (210, 211) directly to said monitoring means (12) or through said interception control means (12).

37. An agent apparatus (22) in a packet-oriented local-area network (40, 41), comprising an interception means (11) for intercepting and copying information from a packet being transmitted in said packet-oriented local-area network (40, 41) and an interception control means (10) for controlling said interception means (11), said interception means (11) comprises a program module (11") stored in a first memory means (250, 251) associated with a first processing unit (240) and a main part (11') stored in a second memory means (252, 253) associated with a second processing unit (230) and said agent apparatus (22) being adapted to be connected to at least one monitoring means (12) for monitoring copied information from said packet, where said copied information is transmitted by said interception means (11) directly to said monitoring means (12) or through said interception control means (10).

38. An agent apparatus (22) according to claim 37, where said interception control means (10) comprises a program module (10") stored in said first memory means (250, 251) associated with said first processing unit (240) and a main part (10') stored in said second memory mean (252, 253) associated with said second processing unit (230).

39. An agent computer program (60, 61) comprised in a local-area network (40, 41), comprising computer readable code means for simplifying firewall definitions and terminating communication between said local-area network (40, 41) and another network, said agent computer program (60, 61) further comprises an interception

computer program (11) comprising computer readable code means configured to cause an interception and copying of information in a packet being transmitted in said local-area network (40, 41), and computer readable code means configured to allow communication between said interception computer program (11) and an interception control computer program (10) for controlling said interception computer program (11).

40. An agent computer program (60, 61) according to claim 39, where said interception computer program (11) comprises computer readable code means configured to cause a transmission of copied information to a monitoring means (12) for monitoring said copied information.

41. An agent computer program (60, 61) according to claim 39, where said interception computer program (11) comprises computer readable code means configured to cause a transmission of copied information to said interception control computer program (10).

42. A computer program product comprising a computer useable medium (154, 200) and an agent computer program (60, 61) according to claim 39, said agent computer program (60, 61) being recorded on said computer useable medium (154, 200).

43. An interception computer program (11) comprising computer readable code means configured to cause an interception and copying of information in a packet being transmitted in a communications network (40, 41), and computer readable code means configured to allow communication between said interception computer program (11) and an interception control computer program (10) for controlling said interception computer program (11).

44. An interception computer program (11) according to claim 43, comprising computer readable code means configured to cause a transmission of copied information to a monitoring means (12) for monitoring said copied information.

45. An interception computer program (11) according to claim 43, comprising computer readable code means configured to cause a transmission of copied information to said interception control computer program (10).

46. An interception computer program according to claim 43, comprising a program module (11"), which is adapted to be stored in a first memory means (250, 251) associated with a first processing unit (240), and a main part (11') adapted to be stored in a second memory means (252, 253) associated with a second processing unit (230), where said program module (11") comprises said computer readable code means configured to cause an interception and copying of information in said packet being transmitted in said communications network (40, 41) and said main part (11') comprises said computer readable code means configured to allow communication between said interception computer program (11) and said interception control computer program (10).

47. A computer program product, comprising a computer useable medium (152, 153, 154, 200) and an interception computer program (11) according to claim 43, said interception computer program (11) being recorded on said computer useable medium (152, 153, 154, 200).

48. An interception control computer program (10) comprising:
computer readable code means configured to cause a controlling of at least one interception computer program (11), which intercept and copy information in a packet being transmitted in a packet-oriented network (1);
computer readable code means configured to enable communication between said interception control computer program (10) and a monitoring means (12) for monitoring copied information from said packet;
computer readable code means configured to enable communication between said interception control computer program (10) and a node (9, 22); and

computer readable code means configured to cause an order to said node (9) or said interception computer program (11) to prevent or terminate communication between user identities where one of said user identities is stored in said interception control computer program (10).

49. An interception control computer program (10) according to claim 48, comprising a computer readable code means configure to cause a transmission of interception related information, such as a call identifier, user identities, addresses associated with said user identities and service information, to said monitoring means (12).

50. An interception control computer program (10) according to anyone of claims 48-49, comprising computer readable code means configured to enable a storage of at least one user identity, whose communication with other user identities shall be intercepted, in said interception control computer program (10).

51. An interception control computer program (10) according to claim 48, comprising computer readable code means configured to cause a positive or negative answer to an interception request from said node (9) of whether a packet related to a user identity connected to said node (9) shall be intercepted.

52. An interception control computer program (10) according to anyone of claims 48-51, comprising computer readable code means configured to cause a reception of said copied information transmitted by said interception computer program (11) and then transmitting said copied information to said monitoring means (12).

53. An interception control computer program (10) according to anyone of claims 48-52, comprising computer readable code means configured to cause a stop signal, which is being transmitted to said interception computer program (11) in order to stop the interception and copying of said packet.

54. An interception control computer program (10) according to anyone of claims 48-53, comprising computer readable code means configured to cause encrypting of all information that is transmitted by said interception control computer program (10).

55. An interception control computer program (10) according to anyone of claims 48-54, comprising a program module (10"), which is adapted to be stored in a first memory means (250, 251) associated with a first processing unit (240), and a main part (10') adapted to be stored in a second memory means (252, 253) associated with a second processing unit (230), where said program module (10") comprises a part of said computer readable code means and the rest of said computer readable code means is comprised in said main part (10').

56. A computer program product comprising a computer useable medium (150, 200) and an interception control computer program (10) according to claim 48, said interception control computer program (10) being recorded on said computer useable medium (150, 200).

Fig. 1

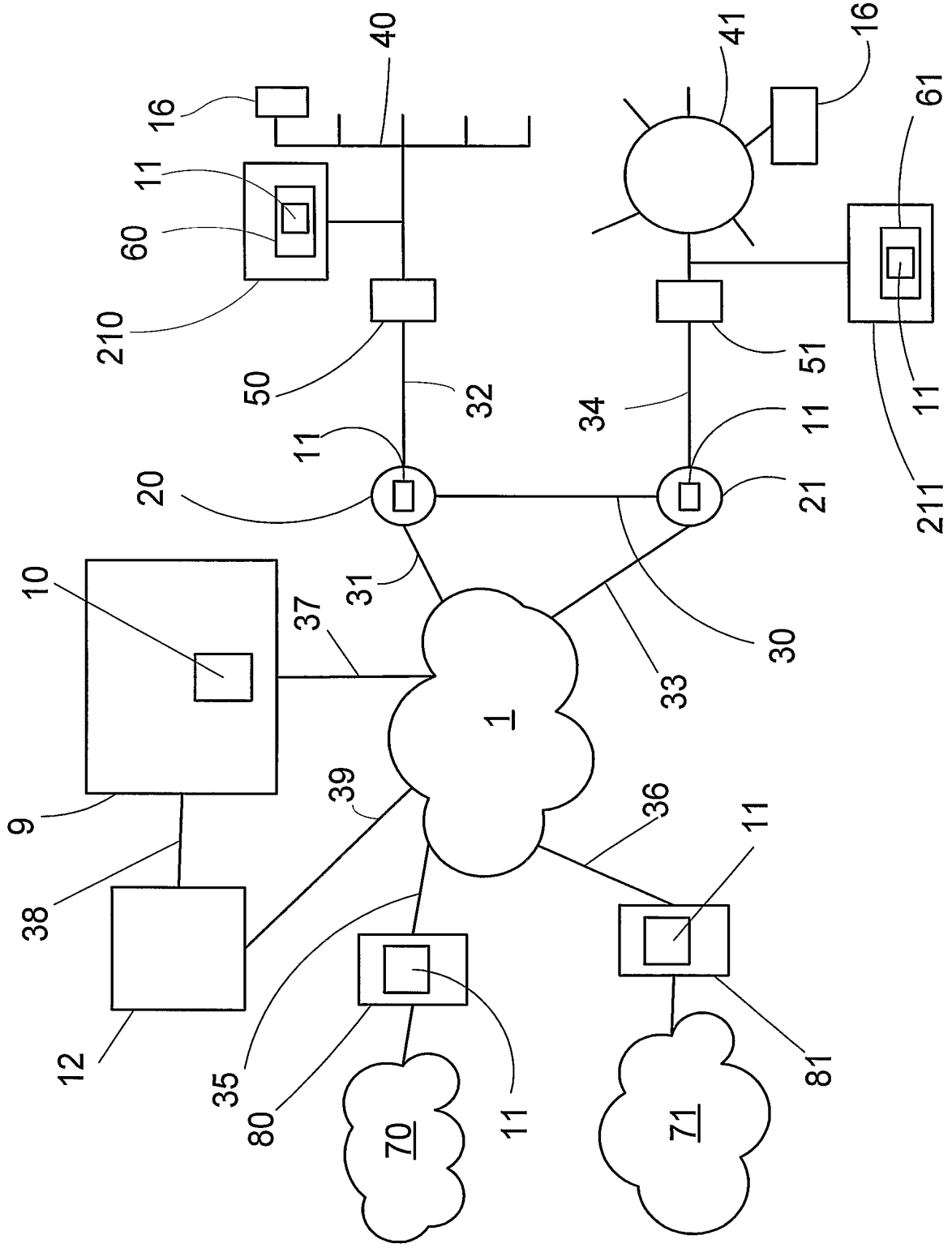

40
16
41
16
61
11
60
210
50
32
34
51
11
11
11
20
21
211
10
37
31
30
1
33
9
39
36
11
38
12
35
80
70
11
71
81

Fig. 2

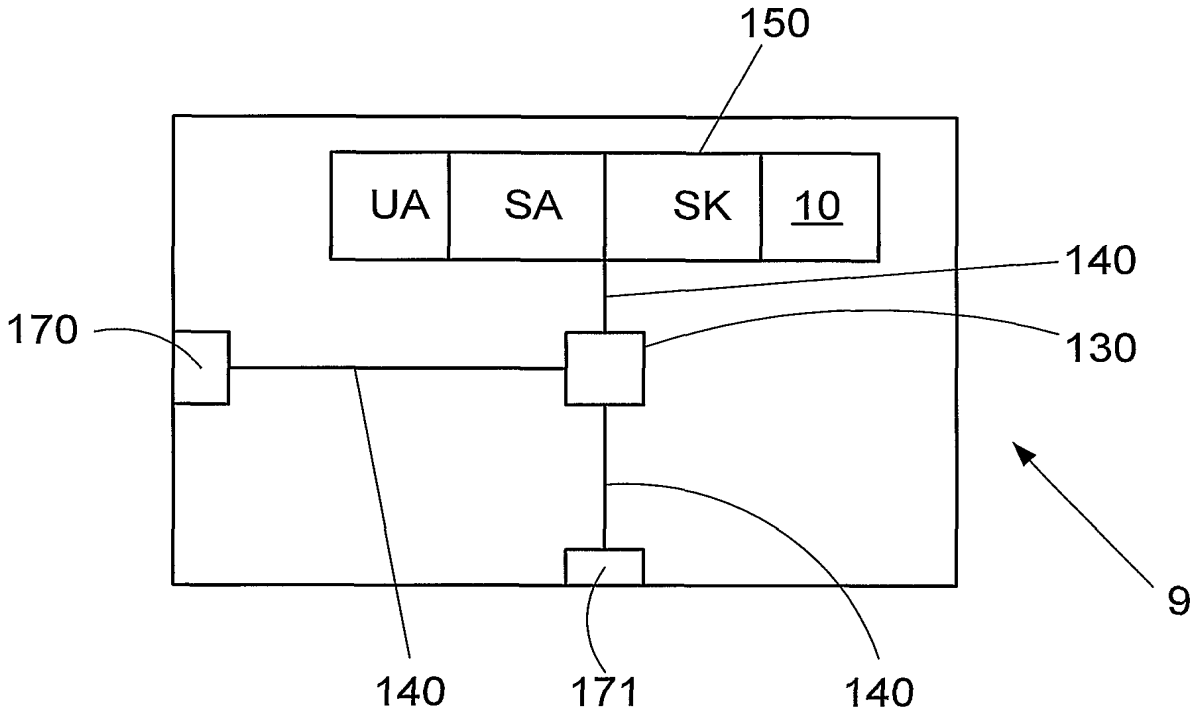

150
UA
SA
SK
10
140
170
130
9
140
171
140

Fig. 3

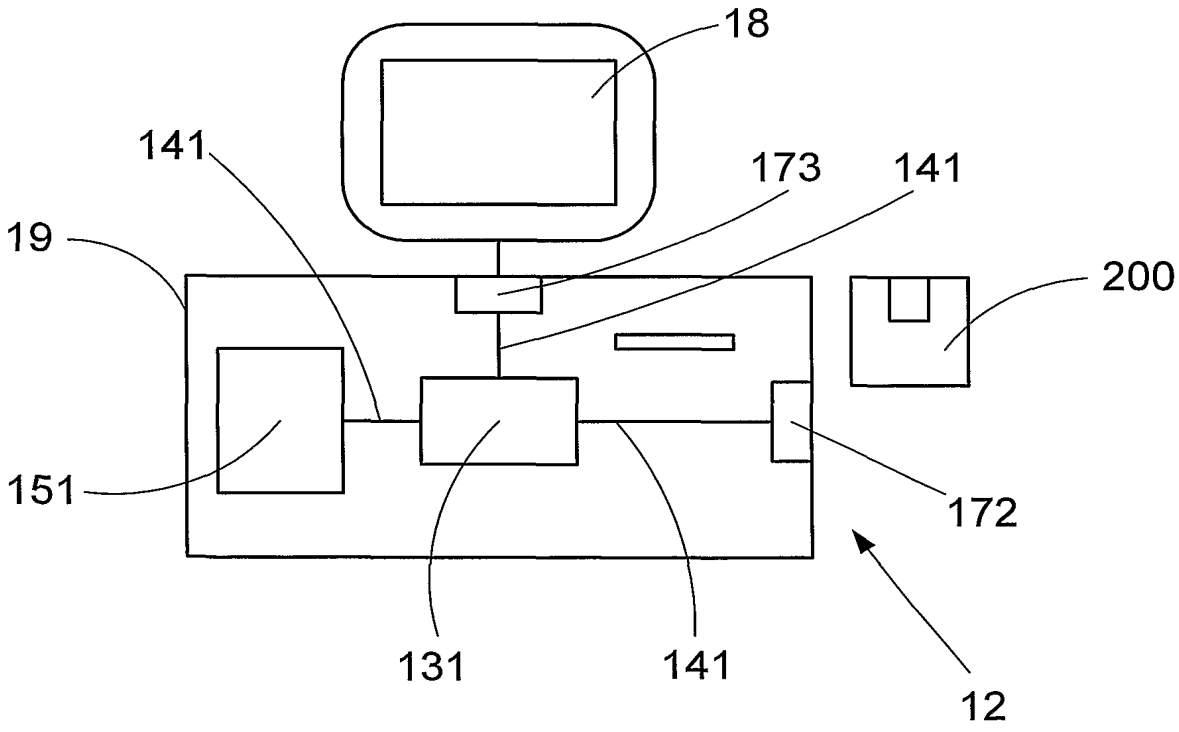

18
141
173
141
19
200
151
172
131
141
12

Fig. 4

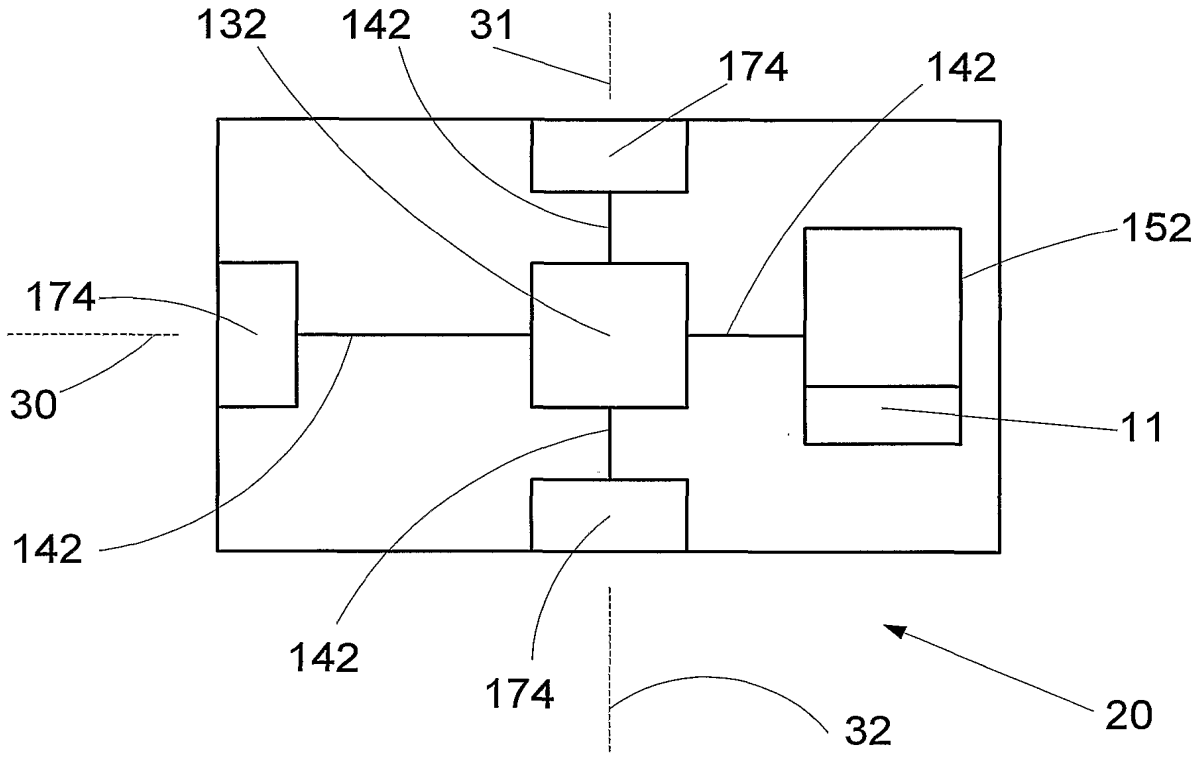

132
142
31
174
142
152
174
30
11
142
142
174
32
20

Fig. 5

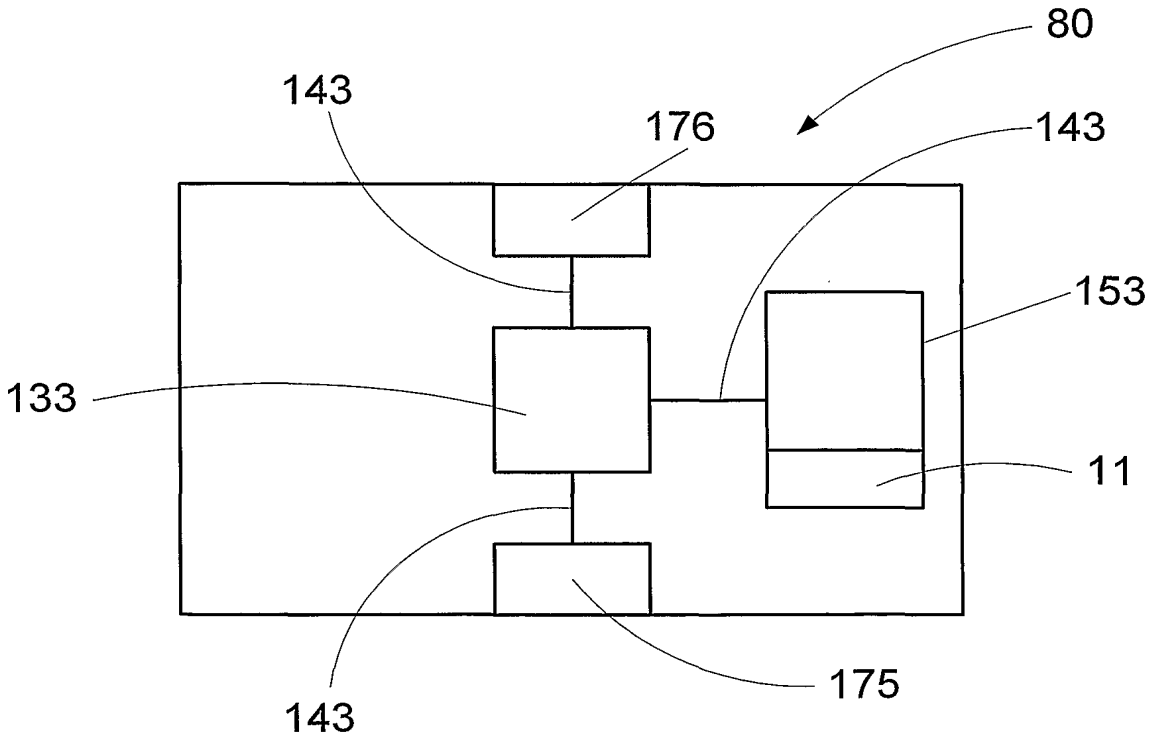
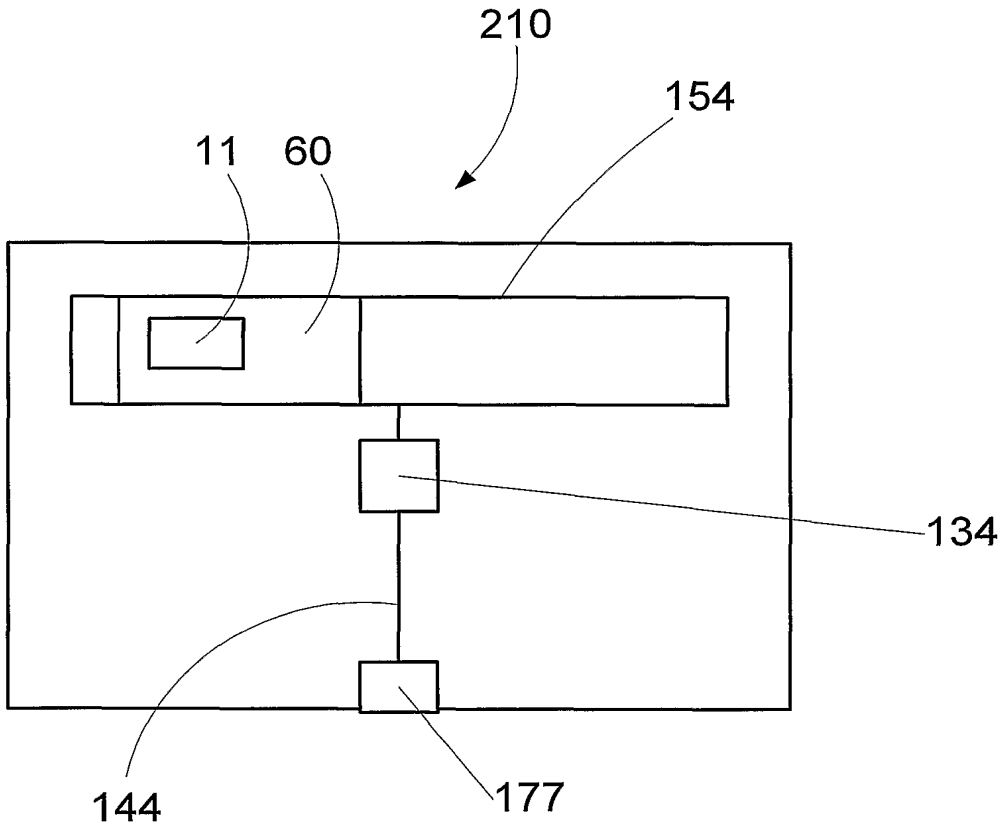

80
143
176
143
153
133
11
143
175

Fig. 6



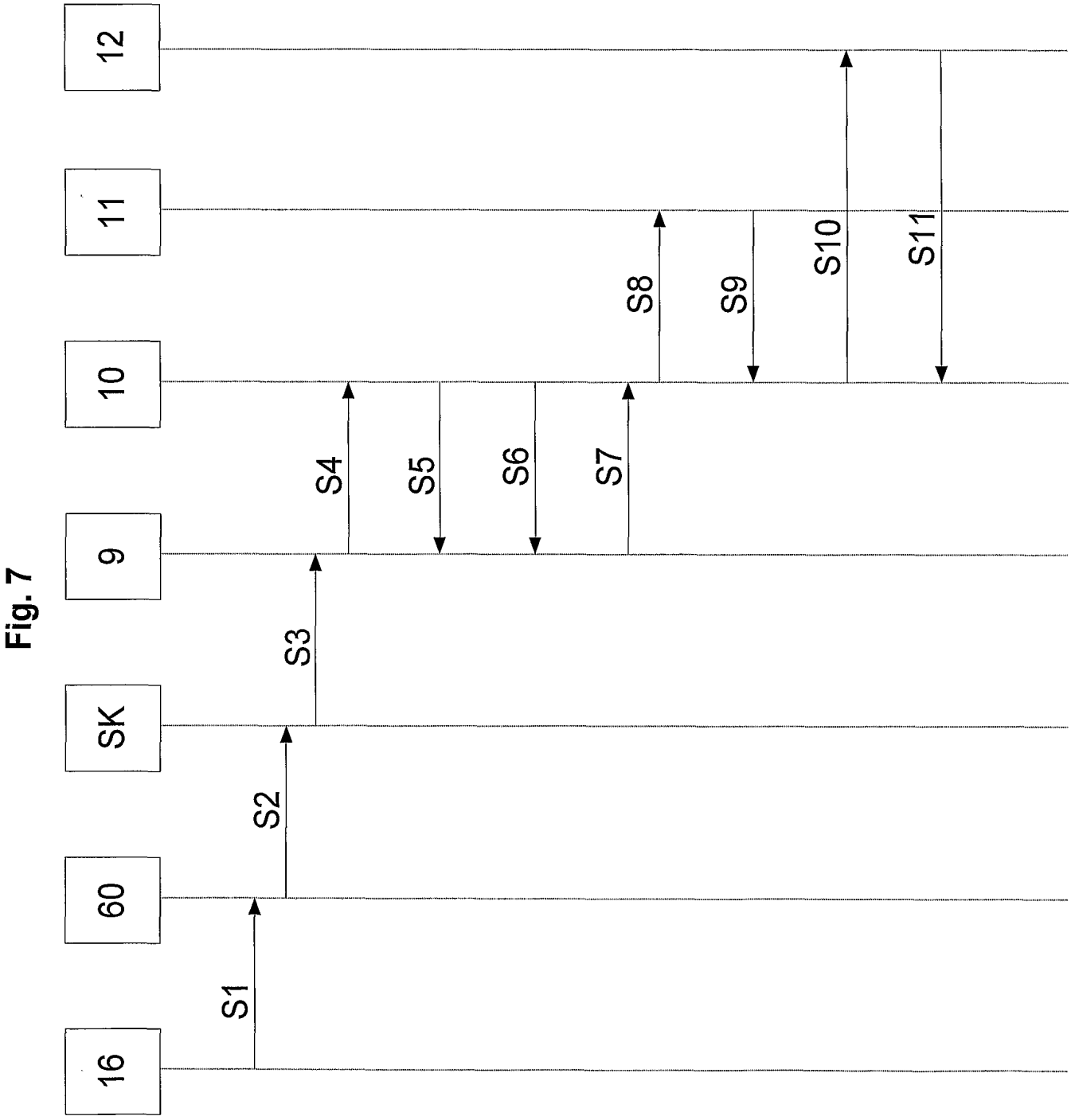


Fig. 7

Fig. 8

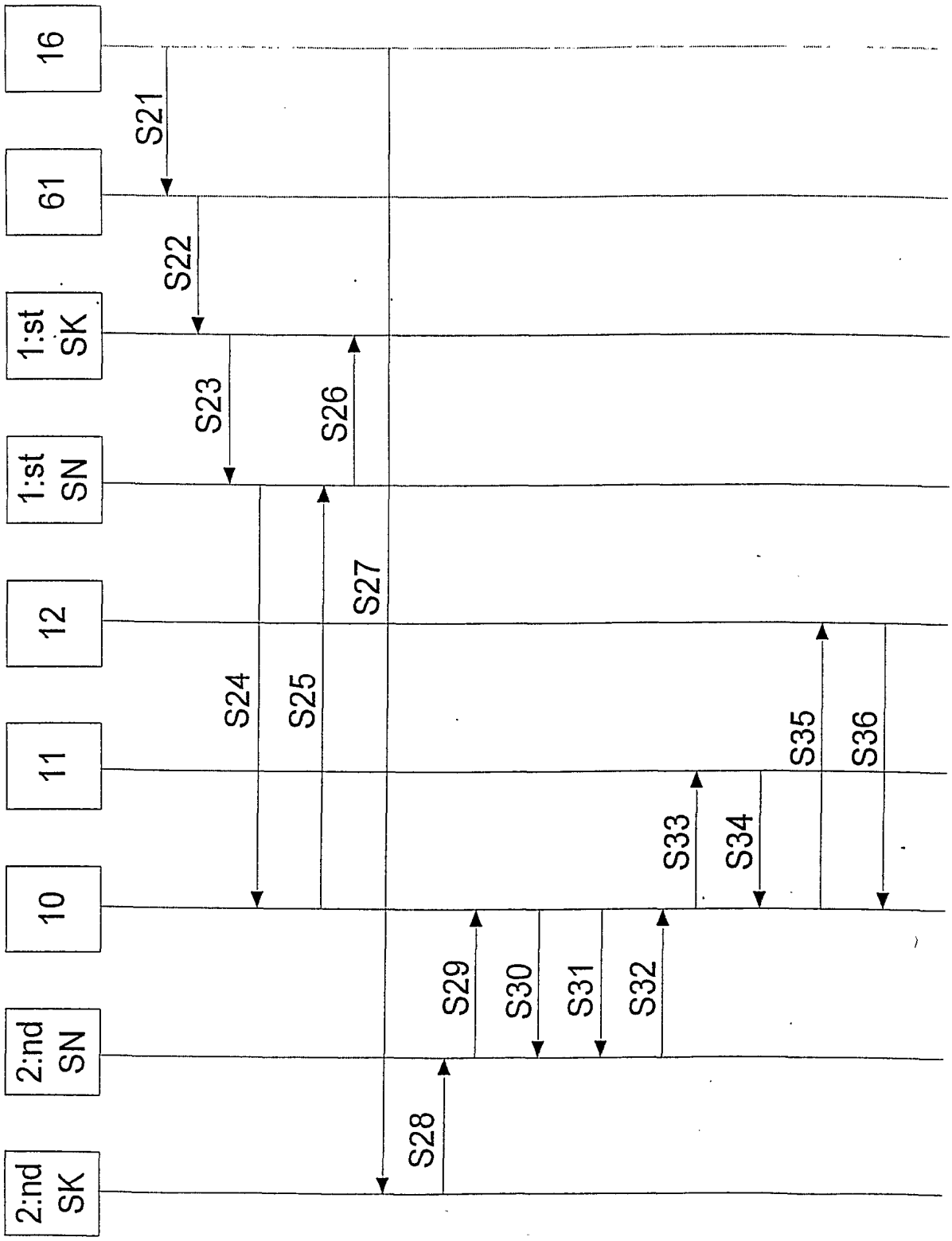
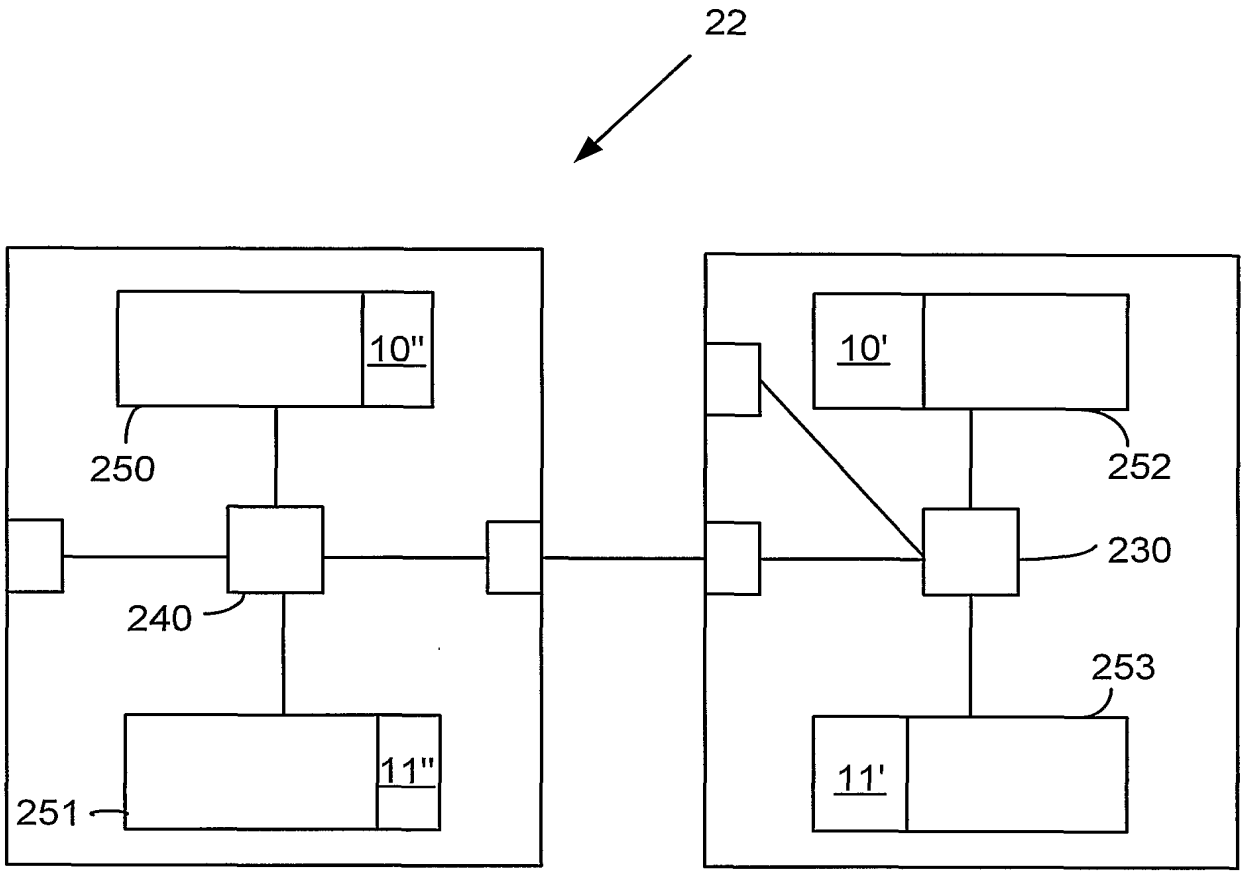

16
61
1:st SK
1:st SN
12
11
10
2:nd SN
2:nd SK
S21
S22
S23
S26
S24
S25
S27
S35
S36
S33
S34
S29
S30
S31
S32
S28

Fig. 9



INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01144

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/26, H04L 12/56, H04L 29/06, H04Q 11/04
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04M, H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INSPEC, WPI DATA, EPO-INTERNAL, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5710971 A (ARMBRUSTER,P.J. ET AL.), 20 January 1998 (20.01.98), column 3, line 10 - column 9, line 67, figures 2,3 --	1-50,54-56
Y	WO 9929089 A1 (MOTOROLA,INC.), 10 June 1999 (10.06.99), page 7, line 21 - page 18, line 30, figures 1-3,5 --	1-50,52, 54-56
A	YEN,s.l. et al: Intelligent MTS monitoring system. In:Security Technology,1994. Proceedings. IEEE, 28th Annual 1994 International Confenece on. On pages 185-187. 12-14 october 1994. ISBN 0-7803-1479-4 --	1-56

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 Sept 2001	20-09-2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Marianne Norrgren/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01144

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9917499 A2 (NOKIA TELECOMMUNICATIONS OY), 8 April 1999 (08.04.99) --	1-56
E,X	WO 0042742 A1 (NOKIA NETWORKS OY), 20 July 2000 (20.07.00) --	1-56

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/08/01

International application No.
PCT/SE 01/01144

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5710971 A	20/01/98	NONE	
WO 9929089 A1	10/06/99	US 6131032 A	10/10/00
WO 9917499 A2	08/04/99	AU 9351598 A	23/04/99
		CN 1277771 T	20/12/00
		EP 1018241 A	12/07/00
		FI 106509 B	00/00/00
		FI 973806 A	27/03/99
WO 0042742 A1	20/07/00	AU 2617399 A	01/08/00